



VMware NSX-T Data Center 2.3 版本說明

VMware NSX-T Data Center 2.3 | 2018 年 9 月 18 日 | 組建編號 10085361

請定期查看這些版本說明的增補和更新。

版本說明的內容

此版本說明涵蓋下列主題：

- [新增功能](#)
- [相容性和系統需求](#)
- [一般行為變更](#)
- [API 參考資訊](#)
- [已解決的問題](#)
- [已知問題](#)

新增功能

NSX-T Data Center 2.3 是累加式升級版本，可增強針對雲端和容器提供的全新多 Hypervisor 平台。

NSX-T Data Center 2.3 版本中提供了下列新功能和增強功能。

NSX-T Data Center 的裸機主機支援簡介

裸機支援包括裸機伺服器上執行的 Linux 系統的工作負載，及沒有 Hypervisor 的裸機伺服器上執行的容器。NSX-T Data Center 利用 Open vSwitch，使任何 Linux 主機成為 NSX-T Data Center 傳輸節點。

- **裸機伺服器支援：**包括執行 RHEL 7.4、CentOS 7.4 和 Ubuntu 16.0.4 作業系統的原生計算工作負載，以允許使用者透過 VLAN 執行網路裸機計算工作負載、覆疊支援的連線，以及針對虛擬-實體和實體-實體通訊流程強制執行微分割原則 (可設定狀態的第 4 層強制執行)。
- **裸機 Linux 容器支援：**在具有 RHEL 7.4 或 RHEL 7.5 的裸機 Linux 主機上使用 RedHat OpenShift Container Platform 執行 Docker 容器。

NSX Cloud 增強功能

- **支援 AWS 部署：**NSX Cloud 對 AWS 工作負載的支援。
- **在 Azure VNET 中自動佈建 NSX 代理程式**
- **內部部署到公有雲之間的 VPN 支援：**包含使用 API 的 NSX Cloud 公有雲間道內的內建 VPN 功能。您可以使用 VPN 功能在下列項目之間建立 IPSEC 連結：
 - 受管理的計算 Amazon VPC/Azure VNet 和第三方服務虛擬機器傳送中的 Amazon VPC/Azure VNet
 - 受管理的 Amazon VPC/Azure VNET 和內部部署 VPN 裝置
- **NSX Cloud 代理程式的擴充作業系統支援：**NSX Cloud 支援公有雲中的 RHEL 7.5 作業系統。

安全服務支援

在路由層的服務插入簡介

- 第 0 層和第 1 層路由器上的服務插入支援：能夠使第三方安全性解決方案上線、在第 0 層和/或第 1 層部署高可用性第三方安全性解決方案，以及透過重新導向原則插入第三方安全性解決方案。
查看《VMware 相容性指南》–〈網路與安全性〉中的 NSX-T Data Center 上第三方解決方案的最新認證狀態。

分散式防火牆增強功能

- NSX Edge 防火牆中的多個區段支援：在 NSX Edge 防火牆中新增多個區段以便易於管理
- 防火牆規則叫用計數和規則權數索引：監控規則使用率和快速識別未使用的規則以便清除
- 防火牆區段鎖定：可讓多個安全管理員在防火牆上同時運作
- 群組物件：如果物件符合所有五個指定的標記 (先前是兩個標記)，則支援將其新增到群組
- 標籤長度：增加標籤長度值 (從 65 到 256) 和標籤範圍 (從 20 到 128)
- 應用程式探索：探索和分類 (也允許使用者自訂分類) 安裝在客體虛擬機器中的應用程式。應用程式將包含有關可執行檔、雜湊、發佈者資訊，以及安裝日期的詳細資料。

網路和 NSX Edge 服務支援

- 在 N-VDS 中對增強型資料路徑模式的覆疊支援：與 vSphere 6.7 搭配使用時，在適用於 NSX-T Data Center 2.3 的 N-VDS 中，增強型資料路徑模式支援需要高效能資料路徑的 NFV 樣式工作負載。
- 在集中式服務連接埠上支援可設定狀態的 NAT 和防火牆服務
- API 支援清除 DNS 轉寄站上的所有 DNS 項目：可在單一 API 呼叫中清除指定 DNS 轉寄站上的所有 DNS 快取項目。在 DNS 伺服器給出錯誤回答時此命令很有用，可避免在修正 DNS 伺服器後等待 DNS 項目逾時。
- 負載平衡器增強功能
 - 支援預先定義的加密清單：用於 HTTPS VIP 之預先定義的 SSL 設定檔，可提高安全性或效能。
 - 負載平衡器規則增強功能：新負載平衡器規則：[刪除標頭動作]、[SSL 相符條件]，以及 [在相符條件中指派變數]。
 - 獨立服務路由器上的負載平衡器支援：能夠在沒有路由器連接埠的服務路由器上部署負載平衡服務。

使用者介面增強功能

- 新語言支援：使用者介面現在提供英文、德文、法文、日文、簡體中文、韓文、繁體中文和西班牙文版本。
- 增強型導覽和首頁：新首頁反白顯示系統的搜尋和快速瀏覽摘要。
- 增強型搜尋：搜尋包括輸入提示 (type-ahead) 建議，可從首頁存取。
- 網路拓撲視覺化：NSX Policy Manager 能夠監控群組至群組、虛擬機器至虛擬機器，以及程序至程序之通訊。您可以視覺化邏輯交換器、連接埠、路由器和 NSX Edge 等網路物件之間的關係。

作業和疑難排解支援

- 安裝和升級增強功能
 - 無狀態的 vSphere 環境中的 NSX-T Data Center：透過為使用 vSphere Auto Deploy 和主機設定檔的無狀態 ESXi 主機提供支援，以啟用其他部署選項。此功能支援需要 vSphere 6.7 U1 或更高版本。
 - 支援 NSX Edge 虛擬機器和裸機同時存在於相同的 NSX Edge 叢集中：NSX Edge 節點虛擬機器和裸機現在可以存在於相同的 NSX Edge 叢集中，以簡化 NSX Edge 節點上主控的服務調整，例如負載平衡器。
 - 模組化 NSX-T Data Center 升級：包括支援升級協調器中的模組化升級。您可以僅升級在新版本中已變更的 NSX-T Data Center 元件。此新增功能可減少修補 NSX-T Data Center 版本的運作額外負荷。
- 監控和疑難排解
 - 用於 KVM Hypervisor 的 ERSPAN：包括對 KVM 上連接埠鏡像的支援 - ERSPAN 類型 II 和 III。
 - 使用 Traceflow 進出第 0 層邏輯路由器上行：能夠從第 0 層邏輯路由器上行產生 Traceflow 流量，報告在第 0 層邏輯路由器上行接收的 Traceflow 封包，以簡化疑難排解作業，並在 Traceflow 報告中包含 NSX Edge 節點的北向介面。
 - CLI 支援在裸機 Edge 節點上關閉 DPDK 連接埠：提供關閉在裸機 NSX Edge 節點上由 DPDK 宣告的連接埠的能力，以簡化在安裝和疑難排解作業期間的連接埠隔離。

OpenStack Neutron 外掛程式支援

在 OpenStack Upstream Queens 版本之前，支援這些功能。

- 可讓 Neutron 外掛程式佈建增強型資料路徑支援的覆疊邏輯交換器：NSX Neutron 外掛程式能夠將增強型資料路徑模式用於覆疊，其過去僅是 VLAN。有了此支援，除了用於執行個體的 OpenStack 環境之外，您還可以將增強型資料路徑效能用於 NFV 相關的工作負載。
- 支援 NSX 產品與 OpenStack 並存：NSX Neutron 外掛程式現在支援同時管理 NSX Data Center for vSphere 和 NSX-T Data Center，用於 OpenStack 實作。
- 可在 OpenStack 中耗用 VPN 即服務功能：在引入了 VPN 功能集的 OpenStack 中，支援 Neutron 延伸中的 OpenStack VPNaaS。

NSX Container Plug-in (NCP) 支援

- 安裝 NSX-T Data Center 的匯合管線
- 負載平衡器 SNAT IP 的註解：在類型為 LoadBalancer 的 Kubernetes 服務中，為負載平衡器的 SNAT IP 加上註解，`ncp/internal_ip_for_policy`: `<SNAT IP>`，並新增到服務的狀態，`status.loadbalancer.ingress.ip`: [`<SNAT IP>`, `<Virtual IP>`]。此 IP 可用於建立允許此 IP CIDR 的網路原則。
- Kubernetes 網路原則增強功能：透過 Kubernetes 網路原則規則，提供從不同命名空間選取網繭的能力。
- Kubernetes 負載平衡器/SNAT 註解改進
 - 如果 NCP 無法設定服務的負載平衡器，將使用 `ncp/error.loadbalancer` 為服務加上註解。
 - 如果 NCP 無法設定服務的 SNAT IP，將使用 `ncp/error.snat` 為服務加上註解。
- 用於 Kubernetes 入口和 OpenShift 路由的 NSX-T Data Center 負載平衡器的工作階段持續性
- 清理指令碼增強功能

相容性和系統需求

如需相容性和系統需求資訊，請參閱 [《NSX-T Data Center 安裝指南》](#)。

無狀態的 vSphere 環境中的 NSX-T Data Center - 若為使用 vSphere Auto Deploy 和主機設定檔的無狀態 ESXi 主機，需求為 vSphere 6.7 U1 或更高版本。

NCP 相容性需求：

產品	版本
NCP/NSX-T Data Center Tile for PAS	2.3.0
NSX-T Data Center	2.2、2.3
Kubernetes	1.10、1.11
OpenShift	3.9、3.10
Kubernetes 主機虛擬機器作業系統	Ubuntu 16.04、RHEL 7.4、7.5
OpenShift 主機虛擬機器作業系統	RHEL 7.4、RHEL 7.5
PAS (PCF)	OpsManager 2.1.x + PAS 2.1.x (PAS 2.1.0 除外) OpsManager 2.2.0 + PAS 2.2.0

一般行為變更

第 1 層邏輯路由器的預設 HA 模式從先佔式變更為非先佔式

在建立第 1 層邏輯路由器時，預設 HA 模式為先佔式，慣用 NSX Edge 節點重新上線時導致流量下降。新預設 HA 模式為非先佔式後，新建立的第 1 層邏輯路由器不會遇到此流量下降。現有的第 1 層邏輯路由器不會受此變更影響。

從傳輸節點到 NSX Controller 的通訊變更

由於從傳輸節點到 NSX Controller 的通訊發生變更，您現在必須針對 NSX-T 2.2 及更高版本開啟 TCP 連接埠 1235。請參閱 [《NSX-T 安裝指南》](#)。

從 NSX-T 2.1 升級至更高版本時，必須開啟 TCP 連接埠 1234 和 1235。升級完成後，TCP 連接埠 1235 處於使用中。

API 參考資訊

請參閱 [〈NSX-T Data Center 和 NSX 原則已過時的 API 呼叫和內容〉](#)。

最新的 API 參考位於 [〈NSX-T Data Center 產品資訊〉](#) 內。

已解決的問題

已解決的問題分類如下。

- [一般已解決的問題](#)
- [安裝已解決的問題](#)
- [NSX Manager 已解決的問題](#)
- [NSX Edge 已解決的問題](#)
- [邏輯網路已解決的問題](#)
- [安全服務已解決的問題](#)
- [負載平衡器已解決的問題](#)
- [解決方案互通性已解決的問題](#)
- [作業和監控服務已解決的問題](#)
- [升級已解決的問題](#)
- [API 已解決的問題](#)
- [NSX Container Plug-in \(NCP\) 已解決的問題](#)

一般已解決的問題

- 問題 1775315：從網頁瀏覽器開啟 Postman 用戶端時，會發生 CSRF 攻擊
對於使用 Postman、CURL 或其他 REST 用戶端進行的 API 呼叫，您必須明確提供 XSRF-TOKEN 標頭及其值。使用遠端驗證的第一個 API 呼叫或 /api/session/create (本機驗證) 的呼叫在回應物件中承載 XSRF-Token。後續的 API 呼叫在 XSRF-TOKEN 標頭中承載 Token 值做為要求的一部分。
- 問題 1989412：還原連線時，不會反映無法連線到 NSX Manager 時的網域刪除
如果在無法連線到 NSX Manager 時從原則中刪除網域，還原與 NSX Manager 的連線後，防火牆和所刪除網域的對應規則仍然存在。
- 問題 2018478：嘗試從儀表板移除 Widget 會導致當機和堆疊追蹤錯誤
自訂儀表板使用者介面變更 (例如，從多個 Widget 移除 Widget)，導致使用者介面當機和堆疊追蹤錯誤。
- 問題 1959647：使用資料庫伺服器別名名稱建立 DSN 時，可能會造成 vCenter Server 安裝失敗
當您使用資料庫伺服器別名名稱建立 DSN 時，含外部 Microsoft SQL 資料庫的 vCenter Server 安裝會失敗。詳細目錄服務安裝期間會出現下列錯誤：啟動 invsvc 時發生錯誤。

安裝已解決的問題

- 問題 1739120：重新啟動管理平面或管理平面中的 Proton 服務之後，網狀架構節點的部署狀態變得停滯
當您在網狀架構頁面上使用主機認證新增支援的主機時，狀態會變更為安裝進行中。重新啟動管理平面或管理平面中的 Proton 服務之後，主機的部署狀態會無限期顯示安裝進行中或解除安裝進行中。

- 問題 1944669：在 KVM 上部署 NSX-T Data Center 應用裝置需要指定確切的記憶體大小
在 ESX 上部署 NSX-T Data Center 應用裝置時，您可使用不同的 RAM 組態部署小型、中型和大型應用裝置。
但是，在 KVM 上部署 NSX-T Data Center 應用裝置時，必須明確設定 RAM 配置。
- 問題 1944678：部署 NSX-T 整合應用裝置需要有效的角色類型
在 KVM 中部署 NSX-T 整合應用裝置，而無任何指定的角色或含無效的角色類型時，其會以不支援的組態部署，且啟用所有角色。
- 問題 1958308：當主機處於鎖定模式時，主機準備或傳輸節點建立會失敗
當主機處於鎖定模式時，主機準備或傳輸節點建立會失敗出現下列錯誤訊息：**執行此作業的權限遭拒。**

NSX Manager 已解決的問題

- 問題 1954923：管理平面升級期間，連線至邏輯交換器的虛擬機器 vMotion 失敗
升級管理平面時，如果您嘗試對連線到邏輯交換器的虛擬機器執行 vMotion，則 vMotion 會失敗。
- 問題 1954927：NSX Manager 的還原完成，並向 NSX Manager 登錄新的非受 VC 管理 ESX 主機，且其
虛擬機器連線至現有邏輯交換器後，在 ESX 主機的 MOB 上，虛擬機器的 MAC 位址會變成空白
NSX Manager 的還原完成，並向 NSX Manager 登錄新的非受 VC 管理 ESX 主機，且其虛擬機器連線至現有邏
輯交換器後，在 ESX 主機的 MOB 上，虛擬機器的 MAC 位址會變成空白。
- 問題 1978104：在 Internet Explorer 11 上，NSX Manager 使用者介面中的部分頁面無法存取
在 Windows 機器上使用 Internet Explorer 時，NSX Manager 使用者介面中的 [儀表板]、[入門工作流程] 和
[負載平衡器] 頁面無法存取。
- 問題 1954986：當金鑰從 UI 中刪除時，授權金鑰會顯示在記錄中
NSX 授權金鑰顯示在 /var/log/syslog 中，如下所示：

```
<182>1 2017-03-24T05:03:47.008Z bb-mgr-221 NSX - SYSTEM [nsx@6876 audit="true"
comp="nsx-manager" reqId="3d146f2b-fa34-460f-8ac3-56e3c7326015"
subcomp="manager"] UserName:'admin', ModuleName:'License',
Operation:'DeleteLicense, Operation status:'success', New value: ["
<license_key>"] <182>1 2017-03-24T05:03:47.009Z bb-mgr-221 NSX - - [nsx@6876
audit="true" comp="nsx-manager" subcomp="manager"] UserName:'admin',
ModuleName:'Batch', Operation:'RegisterBatchRequest, Operation status:'success',
New value: [{"atomic":false} {"request":
[{"method":"DELETE","uri":"/v1/licenses/<license_key>"}]}]
```

如果將應用裝置設定為傳送記錄給外部記錄收集器，則外部記錄收集器上任何已獲得授權的使用者也能看到金鑰值。

- 問題 1956055：當管理平面資料存放區關閉時，本機管理員使用者無法從 UI 存取技術支援服務包
當管理平面資料存放區關閉時，本機管理員使用者無法從 UI 存取技術支援服務包。
- 問題 1957165：載入搜尋結果集 (擁有 10,040 或更多個記錄) 的最後一頁會導致錯誤
針對根據搜尋查詢可傳回 10,040 或更多個物件的大型環境，嘗試載入結果集的最後幾個記錄時，您可能會看到錯誤。

NSX Edge 已解決的問題

- 問題 1762064：在將 NSX Edge 重新開機後立即設定 NSX Edge VTEP IP 集區和上行設定檔，會導致
VTEP BFD 工作階段成為無法聯繫的狀態
將 NSX Edge 重新開機後，代理需要一些時間才能重設 NSX Edge 連線。

邏輯網路已解決的問題

- 問題 1966641：新增主機並將其設定為傳輸節點後，如果該節點不屬於邏輯交換器，其狀態會顯示為

[關閉]

新增主機並將其設定為傳輸節點後或設定至 NSX-T 2.1 的升級計劃時，如果傳輸節點不屬於邏輯交換器，在使用者介面其狀態會顯示為 [關閉]。

- 問題 2015445：作用中服務路由器上的防火牆狀態可能不會在新的作用中服務路由器上複製
承租人邏輯路由器 (TLR) 可能有多個從 NSX Edge1 至 NSX Edge2 以及從 NSX Edge2 至 NSX Edge1 的容錯移轉。防火牆或 NAT 流程狀態會在作用中/待命 TLR 服務路由器之間同步。在非先佔式容錯移轉模式下設定 TLR 時，同步會在第一個容錯移轉之前發生，但不會在第一個容錯移轉與後續容錯移轉之間發生。因此，在第二個容錯移轉時，TCP 流量會逾時。在先佔式模式下設定的 TLR 不會發生此問題。
- 問題 2016629：移轉後，RSPAN_SRC 鏡像工作階段會失敗
當連線到為 RSPAN_SRC 鏡像工作階段指派的連接埠的虛擬機器移轉至另一個 Hypervisor，並且目的地 Hypervisor 的目的地網路上沒有所需的 pNic 時，將無法在連接埠上設定 RSPAN_SRC 鏡像工作階段。此失敗會導致連接埠連線失敗，但 vMotion 移轉程序會成功完成。
- 問題 1620144：即使在傳輸節點遭刪除後，NSX-T Data Center CLI **get logical-switches** 仍會列出狀態為「啟動」的邏輯交換器
CLI 可能會讓使用者誤認為有可運作的邏輯交換器。即使有邏輯交換器顯示出來，實際上卻是無法運作的。傳輸節點被刪除後，會停用不透明交換器，因此不會有任何流量通過。
- 問題 1590888：需要有警告指出在 [乙太網路] 區段中選取的邏輯連接埠只會套用於相同的 L2 網路內
對於分散式防火牆，在 [乙太網路] 區段中，如果在來源/目的地區段中輸入了任何邏輯連接埠或 MAC 位址，則應有警告指出 MAC 位址或邏輯連接埠應屬於相同 L2 網路 (連結至相同邏輯交換器) 的虛擬機器連接埠。目前並沒有警告訊息。
- 問題 1763576：即使 Hypervisor 在 NSX-T Data Center 網路上有虛擬機器，仍可將其視為傳輸節點而移除
即使在屬於 NSX-T Data Center 網路的節點上有虛擬機器，NSX-T Data Center 也不會阻止您刪除傳輸節點。刪除傳輸節點後，虛擬機器會失去連線。
- 問題 1780798：在大規模環境中，部分主機可能會進入失敗狀態
在主機節點數大於或等於 200 的大規模環境中，在執行一段時間之後，部分主機可能會失去與 NSX Manager 的連線，且記錄會包含如下的錯誤訊息：
2016-12-09T00:57:58Z mpa: [nsx@6876 comp="nsx-esx" subcomp="mpa" level="WARN"]
Unknown routing key: com.vmware.nsx.tz.*
- 問題 1954997：如果在刪除傳輸節點時，傳輸節點上的虛擬機器連線至邏輯交換器，傳輸節點刪除會失敗
 1. 建立網狀架構節點和傳輸節點。
 2. 將 VIF 連結至邏輯交換器。
 3. 如果不移除 VIF 與邏輯交換器的連結，則刪除傳輸節點會失敗。
- 問題 1958041：當 ESX Hypervisor 具有多個上行時，BUM 流量對實體第 2 層區段的第 3 層流量可能無法正常運作
如果符合下列所有條件，則來自邏輯路由器中來源 Hypervisor 的 BUM 流量可能不會到達目的地 Hypervisor。
 - ESX 具有多個上行
 - 來源和目的地虛擬機器透過邏輯路由器連線
 - 來源和目的地 Hypervisor 位於不同的實體區段
 - 目的地邏輯網路使用 MTEP 複寫發生此情況的原因是 BFD 模組可能尚未建立工作階段，這表示目的地邏輯網路的 MTEP 選取可能尚未發生。

- 問題 1520694：在 RHEL 7.1 核心 3.10.0-229 和較舊版本中，FTP ALG 無法在資料通道上開啟交涉的連接埠
對於 FTP 工作階段 (用戶端和伺服器都位於相同 Hypervisor 上的虛擬機器中)，FTP 應用程式層級閘道 (ALG) 不會開啟資料通道的交涉連接埠。這是 Red Hat 才會有的問題，出現在 RHEL 7.1 核心 3.10.0-229 中。較新的 RHEL 核心不受影響。
- 問題 2008882：要使 Application Discovery 正常運作，不要建立跨多台主機的安全群組
如果一個安全群組具有跨多台主機的虛擬機器，Application Discovery 工作階段可能會失效。

負載平衡器已解決的問題

- 問題 1995228：組態變更和重新載入後，加權循環配置資源和加權最少連線演算法可能不會正確散佈流量
加權循環配置資源或加權最少連線組態發生變更並重新載入時，伺服器會中斷連線。連線中斷後，不會保留歷史流量散佈資訊，這將導致無法正確散佈流量。
- 問題 2018629：健全狀況檢查資料表不顯示 NS 群組集區已更新的監控類型
當您使用相同的成員和一種監控類型建立靜態和動態 NS 群組集區，並變更動態集區上的該監控類型時，動態集區健全狀況檢查不會出現在健全狀況檢查資料表中。
- 問題 2020372：達到失敗計數上限後，被動健全狀況檢查不會將集區成員考慮在內
被動健全狀況檢查需要比設定計數更多的失敗計數值，才會將集區成員考慮在內。

解決方案互通性已解決的問題

- 問題：2025624：載入時 Splunk 儀表板停滯或儀表板上的圖表為空白
由於 HTML 範本錯誤地指向查詢指令碼的先前路徑，因此 Splunk 會擷取舊版 *nsx_splunk_app*。這樣一來，儀表板會執行包含諸如 *vmw_nsxt_comp*、*vmw_nsxt_subcomp* 和 *vmw_nsxt_errorcode* 等欄位的舊查詢，這些欄位在更新版本的查詢指令碼中以不同方式命名。因此，查詢會傳回空結果，且儀表板會保留空白。

作業和監控服務已解決的問題

- 問題 1957092：由於在載入 Docker 映像時發生錯誤而無法初始化 NSX Controller 叢集
`initialize control-cluster` 命令失敗，並顯示錯誤訊息：**控制叢集啟用逾時。請再試一次。**syslog 中還會顯示下列記錄資訊：

```
<30>1 2017-08-03T22:52:41.258925+00:00 localhost load-zookeeper-image 1183 - -  
grpc: the connection is unavailable.
```

升級已解決的問題

- 問題 1847884：請勿進行 NSX-T Data Center 相關的變更，除非管理平面的升級程序已完成
在管理平面升級期間執行任何變更，例如，建立、更新或刪除傳輸區域、傳輸節點或邏輯交換器，可能會損毀管理平面，導致 NSX Edge、主機和資料路徑連線失效。
- 問題 2005709：當您使用 NSX Manager FQDN 時，升級協調器頁面變得無法存取
當您使用 NSX Manager FQDN 開啟 NSX Manager 使用者介面時，升級協調器頁面中出現下列錯誤訊息：**僅當升級協調器正在執行時，此頁面在 NSX Manager 上才可用。若要啟用服務，請在 NSX Manager 上執行命令「set service install-upgrade enabled」。如果安裝-升級服務已啟用，請先嘗試使用「clear service install-upgrade enabled」將其停用，然後再次將其啟用。**
- 問題 2022609：受管理的主機在升級協調器中被視為未受管理的主機
如果環境中有超過 128 部受管理的主機，升級程序期間屬於叢集的主機會出現在未受管理的 ESXi 群組中。
- 問題 1944731：升級第二個 NSX Edge 期間，如果第一個已升級的 NSX Edge 提供大量要求，則 DHCP 租用可能具有衝突的記錄

升級第二個 NSX Edge 期間，如果第一個已升級的 NSX Edge 提供大量要求，則 DHCP 租用可能具有衝突的記錄。

API 已解決的問題

- 問題 1619450：垂直測試經由輪詢頻率組態 API **GET /api/v1/hpm/features** 而傳回
GET /api/v1/hpm/features 會傳回所有可設定輪詢頻率之功能的清單。此 API 會傳回一些內部的僅限測試功能。除了有雜訊外，使用者的功能不受影響。
- 問題 1781225：API **GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules** 不適用於 Ubuntu
API GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules 適用於 ESXi 和 RHEL，但不適用於 Ubuntu。
- 問題 1954990：傳回不準確的實現 API 狀態
如果使用實現 API 檢查屏障前執行之所有 API 的實現狀態，實現 API 的傳回狀態會與實際狀態產生差異。由於在管理平面中執行 DFW 的程序極為複雜，DFW API 可能會在應該遵循的屏障後發生差錯，因而造成狀態不準確的情形。

NSX Container Plug-in (NCP) 已解決的問題

- 問題 2167491：如果 NSX-T 負載平衡器的虛擬伺服器數目已達上限，則 NCP 無法啟動
在 NCP 的 ConfigMap 中，您可以將 NSX-T 負載平衡器的大小設定為小型、中型或大型。對於小型負載平衡器，虛擬伺服器的數目上限為 10；對於中型負載平衡器，為 100；對於大型負載平衡器，則為 1000。如果負載平衡器的虛擬伺服器數目已達上限，NCP 將不會啟動。若要查看負載平衡器的虛擬伺服器數目是否已達上限，請在 NSX-T Manager GUI 中，找到負載平衡器 (它具有與叢集同名的標籤) 並計算虛擬伺服器數目。
- 問題 2160806：不支援在 NCP 未執行時更新作用中入口的 TLS 規格
如果 NCP 已指派外部 IP 給入口資源，且在 NCP 未執行時您更新入口的 TLS 規格，例如，透過移除或變更參數 secretName，NCP 將感知不到所做的變更。當 NCP 再次執行時，對應至舊密碼的憑證仍存在，並且不會刪除。

已知問題

已知問題分類如下。

- [一般已知問題](#)
- [安裝已知問題](#)
- [NSX Manager 已知問題](#)
- [NSX Edge 已知問題](#)
- [邏輯網路已知問題](#)
- [安全服務已知問題](#)
- [KVM 網路已知問題](#)
- [負載平衡器已知問題](#)
- [解決方案互通性已知問題](#)
- [作業和監控服務已知問題](#)
- [升級已知問題](#)
- [API 已知問題](#)
- [NSX Policy Manager 已知問題](#)
- [NSX Cloud 已知問題](#)
- [NSX Container Plug-in \(NCP\) 已知問題](#)
- [說明文件勘誤與增補](#)

一般已知問題

- 問題 1842511：Multihop-BFD 不支援靜態路由

在 NSX-T 2.0 中，可為 (MH-BGP) Multihop BGP 芳鄰啟用 BFD (雙向轉送偵測)。在 NSX-T 2.0 中無法設定使用 BFD 來支援 Multihop 靜態路由的功能，只有 BGP 可以。請注意，如果您已設定由 BFD 支援的 Multihop BGP 芳鄰，並使用與 BGP 芳鄰相同的 Nexthop 來設定對應的 Multihop 靜態路由，則 BFD 工作階段狀態會同時影響 BGP 工作階段和靜態路由。

因應措施：無。

- 問題 1931707：自動傳輸點功能要求叢集中的所有主機都具有相同的 pnics 設定

自動傳輸點功能要求叢集中的所有主機都具有相同的 pnics 設定。範本中的所有 pnics 必須可供傳輸節點組態的所有主機使用，否則 pnics 遺失或遭佔用之主機上的傳輸節點組態可能失敗。

因應措施：如果傳輸節點組態失敗，請重新設定個別傳輸節點以便更正。

- 問題 1909703：NSX 管理員可在 OpenStack 直接從後端所建立的路由器中建立新的靜態路由、NAT 規則和連接埠

在 NSX-T 2.0 提供的 RBAC 功能中，NSX 管理員無法從 NSX UI/API 直接刪除或修改由 OpenStack 外掛程式所建立的交換器、路由器、安全性群組等資源。這些資源只能由透過 OpenStack 外掛程式所傳送的 API 來加以修改/刪除。此功能有些限制。目前，NSX 管理員只是不能刪除/修改 OpenStack 所建立的資源，但管理員可以在 OpenStack 所建立的現有資源中建立新資源，例如靜態路由、NAT 規則。

因應措施：無。

- 問題 1957072：橋接器節點的上行設定檔應該一律對多個上行使用 LAG

使用未構成 LAG 的多個上行時，流量無法達到負載平衡，且可能無法正常運作。

因應措施：在橋接器節點上針對多個上行使用 LAG。

- 問題 1970750：搭配使用 LACP 與快速計時器的傳輸節點 N-VDS 設定檔不會套用至 vSphere ESXi 主機設定採用快速速率的 LACP 上行設定檔並套用至 NSX Manager 上的 vSphere ESXi 傳輸節點時，NSX Manager 顯示已成功套用此設定檔，但 vSphere ESXi 主機使用的是預設 LACP 緩慢計時器。

在 vSphere Hypervisor 上，當傳輸節點上使用來自 NSX Manager 的 LACP NSX 受管理分散式交換器 (N-VDS) 設定檔時，您無法查看 LACP 逾時值 (SLOW/FAST) 的效果。

因應措施：無。

- 問題 1989407：具有企業管理員角色的 vIDM 使用者無法覆寫物件保護

具有企業管理員角色的 vIDM 使用者無法覆寫物件保護，且無法建立或刪除主體身分識別。

因應措施：以管理員權限登入。

- 問題 2030784：無法使用包含非 ASCII 字元的遠端使用者名稱登入 NSX Manager。

您無法以具有包含非 ASCII 字元之使用者名稱的遠端使用者身分登入 NSX Manager 應用裝置。

因應措施：當您登入 NSX Manager 應用裝置時，遠端使用者名稱應具有 ASCII 字元。

如果在 Active Directory 伺服器中已設定包含非 ASCII 字元的遠端使用者名稱，則可以使用非 ASCII 字元。

- 問題 2111047：NSX-T 2.2 版中的 VMware vSphere 6.7 主機上不支援 Application Discovery

在安全群組 (擁有 vSphere 6.7 主機上執行的虛擬機器) 上執行 Application Discovery 會導致探索工作階段失敗。

因應措施：無

- 問題 2157370：設定含截斷的 L3 交換連接埠分析器 (SPAN) 時，特定的實體交換器會捨棄鏡像的封包
設定含截斷的 GRE/ERSPAN 所屬的 L3 SPAN 時，因為實體交換器原則而會捨棄截斷的鏡像封包。可能的原因是連接埠正在接收封包，其中裝載中的位元組數不等於類型長度欄位。

因應措施：移除 L3 SPAN 截斷組態。

- 問題 216992：含來自其他主機的目的地 MAC 位址 02:50:56:56:44:52 的鏡像封包遭 vSphere ESXi 上行捨棄
當主機從其他主機接收含目的地 MAC 位址 02:50:56:56:44:52 的鏡像封包時，vSphere ESXi 上行會捨棄這些鏡像封包。

因應措施：無

- 問題 2174583：在 [入門] 精靈中，[設定傳輸節點] 按鈕無法在 Microsoft Edge 瀏覽器中正常運作
在 [入門] 精靈中，按一下設定傳輸節點按鈕後，Microsoft Edge 網頁瀏覽器會失敗並顯示發生 JavaScript 錯誤。

因應措施：改用 Firefox 或 Google Chrome 瀏覽器。

安裝已知問題

- 問題 1617459：Ubuntu 的主機組態不支援尋找介面組態檔的來源
如果 pnic 介面不在 /etc/network/interfaces 檔案中，則不會在網路組態檔中正確設定 MTU。因此，傳輸橋接器的 MTU 組態在每次重新開機後都會遺失。

因應措施：將 PNIC 介面組態移至 /etc/network/interfaces

- 問題 1906410：嘗試從 UI 刪除主機，但不先刪除傳輸節點，會導致主機進入不一致的狀態
嘗試從 UI 刪除主機，但不先刪除傳輸節點，會導致主機進入不一致的狀態。如果您嘗試在主機處於不一致的狀態時刪除傳輸節點，則 UI 不允許您刪除此主機。

因應措施：

1. 刪除傳輸節點前，先關閉此傳輸節點上部署的所有承租人虛擬機器的電源。
2. 從傳輸節點中移除傳輸區域。
3. 刪除傳輸節點。
4. 如果已成功刪除傳輸節點，然後再刪除相應的主機。

如果傳輸節點刪除失敗，請完成知識庫 <https://kb.vmware.com/s/article/52068> 中的步驟。

- 問題 1957059：嘗試進行主機取消準備時，如果將包含現有 VIB 的主機新增至叢集，則取消準備會失敗
將主機新增至叢集之前，如果未完全移除 VIB，則主機取消準備作業會失敗。

因應措施：請確定主機上的 VIB 已完全移除，並重新啟動主機。

- 問題 2106956：將屬於相同叢集的兩個 NSX Controller 加入兩個不同的 NSX Manager 會導致未定義的資料路徑問題
將屬於相同 NSX Controller 叢集的兩個 NSX Controller 加入兩個不同的 NSX Manager 會導致未定義的資料路徑問題。

因應措施：在 NSX Manager 上使用中斷連結 CLI 命令，以從 NSX Controller 叢集移除 NSX Controller。重新設定 NSX Controller 叢集，以便叢集中的所有 NSX Controller 均向同一個 NSX Manager 登錄。

請參閱《NSX-T Data Center 安裝指南》。

- 問題 2106973：初始化所有 NSX Controller 上的 NSX Controller 叢集會導致每個 NSX Controller 成為一個節點 NSX Controller 叢集，進而導致發生未定義的資料路徑連線問題
避免初始化所有 NSX Controller 上的 NSX Controller 叢集，其會導致每個 NSX Controller 成為一個節點 NSX Controller 叢集，進而導致發生未定義的資料路徑連線問題。僅初始化第一個 NSX Controller 上的 NSX Controller 叢集，然後在第一個 NSX Controller 上透過執行 `join control-cluster` CLI 命令將其他 NSX Controller 加入叢集。

因應措施：如《NSX-T Data Center 安裝指南》。

- 問題 2114756：在某些情況下，從 NSX-T Data Center 備妥的叢集中移除主機時不會移除 VIB。從 NSX-T Data Center 備妥的叢集中移除主機時，部分 VIB 可能會保留在主機上。

因應措施：從主機手動解除安裝 VIB。

- 問題 2059414：由於 python-gevent RPM 的版本較舊，RHEL LCP 服務包安裝會失敗。如果 RHEL 主機包含較新版本的 python-gevent RPM，RHEL LCP 服務包安裝會失敗，因為 NSX-T Data Center RPM 包含較舊版本的 python-gevent RPM。

因應措施：如果主機包含最新版本的 python-gevent RPM，則在 RHEL 主機上手動安裝 LCP 服務包。

完成下列步驟：

1. 解壓縮 RHEL LCP 服務包。
 2. 導覽至 LCP 服務包資料夾。
 3. 從 LCP 資料夾中刪除 libev、python-greenlet 和 python-gevent RPM。
 4. 安裝剩餘的 RPM。請參閱《NSX-T Data Center 安裝指南》。
- 問題 2142755：OVS 核心模組無法安裝，視正在執行的次要 RHEL 7.4 核心版本而定。無法在執行次要核心 17.1 版或更高版本的 RHEL 7.4 主機上安裝 OVS 核心模組。安裝失敗會使核心資料路徑停止運作，這會導致應用裝置管理主控台變得無法使用。

因應措施：升級 RHEL 7.4 核心版本。使用管理員權限在主機上執行指令碼

`/usr/share/openvswitch/scripts/ovs-kmod-manage.sh`，並重新載入 OVS 核心模組。

NSX Manager 已知問題

- 問題 1950583：系統升級至 NSX-T 2.0.0 後，NSX Manager 已排程的備份可能會失敗。從先前版本升級至 NSX-T 2.0.0 版後，有些 NSX-T 環境無法執行已排程的備份。這個問題是由於舊版到新版的 SSH 指紋格式有所變更。

因應措施：重新設定已排程的備份。

- 問題 1576112：KVM Hypervisor 若位於不同的第 2 層區段中，則需要手動設定閘道。如果您在 NSX Manager 上設定了 IP 集區，並使用該 IP 集區建立傳輸節點，則 Ubuntu KVM 方塊並不會針對在「IP 集區」組態中設定的閘道顯示路由。因此，在不同 L2 區段中的 Hypervisor 上存在的虛擬機器相互間的覆疊流量將會失敗，因為基礎網狀架構主機不知道如何聯繫遠端區段中的網狀架構節點。

因應措施：為閘道新增路由，使其可將流量路由傳送至位於不同區段中的其他 Hypervisor。如果未手動完成此組態，覆疊流量將會失敗，因為網狀架構節點不知道如何聯繫遠端網狀架構節點。

- 問題 1710152：在相容模式中，NSX Manager GUI 無法在 Internet Explorer 11 中運作。

因應措施：移至工具 > 相容性檢視設定，然後確認 Internet Explorer 在相容模式中並未顯示 NSX Manager GUI。

- 問題 2128476：具有超過 500 個主機、1000 個虛擬機器和 10000 個 VIF 之詳細目錄的規模設定，可能會在強制重新開機後花費大約 30 分鐘進行完整同步。NSX Manager 重新開機後，每個主機將與 NSX Manager 同步，以便 NSX Manager 接收主機上最新的資料，其中包括主機上存在的虛擬機器和虛擬機器上存在的 VIF 的相關資訊。對於具有包含超過 500 個主機、1000 個虛擬機器和 10000 個 VIF 之詳細目錄的規模設定，完整同步需要大約 30 分鐘。

因應措施：強制重新開機後，等待最新資訊顯示在 NSX Manager 中。

使用 API `api/v1/fabric/nodes/<nodeid>/status` 檢查指示特定節點的最新同步時間的 `last_sync_time` 內容。

- **問題 1928376：還原 NSX Manager 後，Controller 叢集成員節點的狀態會降級**
如果將 NSX Manager 還原至從叢集卸離此成員節點之前製作的備份映像，控制器叢集成員節點可能會變得不穩定並回報健全狀況狀態已降級。

因應措施：如果叢集成員資格產生變化，請務必製作新的 NSX Manager 備份。

- **問題 1956088：當視圖中的規則集已套用篩選時，如果在儲存至 Manager 之前篩選已取消，則對防火牆 UI 檢視進行的變更可能會遺失**
當視圖中的規則集已套用篩選時，如果在儲存至 Manager 之前篩選已取消，則對防火牆 UI 檢視進行的變更可能會遺失

因應措施：無。

- **問題 1928447：具有重複虛擬通道端點 IP 位址的 Hypervisor 不會登入管理平面節點 Syslog**
具有重複虛擬通道端點 IP 位址的 Hypervisor 不會登入管理平面節點 Syslog。請確定為 Hypervisor 的虛擬通道端點和 NSX Edge 節點的上行介面指派唯一的 IP 位址。

因應措施：無。

- **問題 2125725：還原大型拓撲部署後，搜尋資料變得不同步，且數個 NSX Manager 頁面無回應**
還原具有大型拓撲部署的 NSX Manager 後，搜尋資料變得不同步，且數個 NSX Manager 頁面會顯示錯誤訊息：**發生無法復原的錯誤。**

因應措施：完成下列步驟：

1. 以管理員身分登入 NSX Manager CLI。
2. 重新啟動搜尋服務。

重新啟動服務搜尋

當搜尋服務在背景中完成修正資料差異時，請等待至少 15 分鐘。

- **問題 2128361：用於將 NSX Manager 的記錄層級設定為偵錯模式的 CLI 命令未正常運作**
使用 CLI 命令 `set service manager logging-level debug` 將 NSX Manager 的記錄層級設定為偵錯模式不會收集偵錯記錄資訊。

因應措施：完成下列步驟：

1. 以管理員身分登入 NSX Manager CLI。
2. 執行命令 `st e` 以切換為根使用者。
3. 複製 `log4j2.xml.default` 和 `log4j2.xml` 檔案。

```
cp /opt/vmware/proton-tomcat/conf/log4j2.xml.default /opt/vmware/proton-tomcat/conf/log4j2.xml
```
4. 變更 `log4j2.xml` 檔案的擁有權。

```
chown uproton:uproton /opt/vmware/proton-tomcat/conf/log4j2.xml
```

- **問題 1964681：管理程式 UI 中的 [主機] 索引標籤會將傳輸節點主機的狀態顯示為 [刪除進行中]，即使已刪除主機亦如此**
從管理程式 UI 中的 [網狀架構] > [節點] > [傳輸節點] 索引標籤，您成功刪除傳輸節點主機之後，[主機] 索引標籤仍將主機的狀態顯示為 [刪除進行中]。

因應措施：重新整理瀏覽器。

- **問題 2169998：如果使用的是 Chrome 瀏覽器，您登入 NSX Manager 時清除瀏覽資料會導致管理程式 UI 停止運作**
您使用 Chrome 瀏覽器登入 NSX Manager 後，如果移至瀏覽器設定，並清除所有瀏覽資料，包括所有基本與進階設定，瀏覽器將中斷與 NSX Manager 的連線。

因應措施：登入 NSX Manager 後，請勿清除瀏覽資料。

NSX Edge 已知問題

- 問題 1765087：由 NSX Edge 建立、用以將封包從資料路徑傳輸至 Linux 核心的核心介面，僅支援最多 1600 的 MTU
資料路徑與核心之間的核心介面不支援 Jumbo 框架。超過 1600 的 BGP 封包大小會被 BGP 精靈截斷及捨棄。超過 1600 的 SPAN 封包大小會被截斷，且封包擷取公用程式會顯示警告。裝載不會截斷，且仍然有效。

因應措施：無。

- 問題 1738960：如果 DHCP 伺服器設定檔 NSX Edge 節點取代為其他叢集中的 NSX Edge 節點，由 DHCP 伺服器指定給虛擬機器的 IP 位址即會變更
此問題是由於被取代的節點與新節點之間缺乏協調所致。

因應措施：無。

- 問題 1629542：在單一 NSX Edge 節點上設定轉送延遲，會導致路由狀態顯示錯誤
以單一 NSX Edge 節點的形式 (而非在 HA 配對中) 執行 NSX Edge 時，設定轉送延遲可能會導致路由狀態的報告不正確。在設定轉送延遲後，路由狀態會誤顯示為關閉，此情況會持續直到轉送計時器到期為止。如果路由器收斂已完成，但轉送延遲計時器尚未到期，則由南到北的資料路徑將如預期繼續推移，即使路由狀態報告為關閉亦然。您可安全地忽略此警告。
- 問題 1601425：無法複製已向 NSX Manager 叢集登錄的 NSX Edge 虛擬機器
不支援複製已向 NSX Manager 叢集登錄的 NSX Edge 虛擬機器。此時應部署全新映像。

因應措施：無。

- 問題 1585575：無法在連結至第 0 層路由器的第 1 層路由器上編輯 NSX Edge 叢集詳細資料
如果您在第 1 層邏輯路由器上啟用了 NAT，則必須先指定 NSX Edge 節點或 NSX Edge 叢集，才能將第 1 層路由器連線至第 0 層路由器。NSX 不支援在已連結至第 0 層路由器的第 1 層路由器上編輯 NSX Edge 叢集詳細資料。

因應措施：若要在已連結至第 0 層路由器的第 1 層路由器上編輯 NSX Edge 叢集詳細資料，請從第 0 層路由器中斷第 1 層路由器的連線、進行變更，然後重新連線。

- 問題 1955830：當 NSX Edge 叢集名稱包含高位元或非 ASCII 字元時，從 NSX-T 1.1 升級至 NSX-T 2.0 會失敗
在 NSX-T 1.1 設定中使用高位元或非 ASCII 字元為 NSX Edge 叢集命名時，從 NSX-T 1.1 升級至 NSX-T 2.0 會失敗，並顯示無限迴圈錯誤。

因應措施：在升級之前，將 NSX Edge 叢集重新命名以移除 NSX-T 1.1 設定執行個體上的高位元或非 ASCII 字元。

- 問題 2122332：在某些情況下，SSH 登入裸機 Edge 無法正常運作
有時，SSH 登入裸機 Edge 無法正常運作。

因應措施：開啟命令提示字元並導覽至 iLO 驅動程式。重新啟動 Edge SSH 服務。

- 問題 2187888：從 NSX Manager 使用者介面自動部署的 NSX Edge 會無限期保持登錄擱置中狀態
從 NSX Manager 使用者介面自動部署的 NSX Edge 會無限期保持登錄擱置中狀態。此狀態會導致 NSX Edge 變得無法用於進一步設定。

因應措施：透過 NSX Manager 使用 CLI 手動登錄 NSX Edge。

邏輯網路已知問題

- 問題 1769922：在 vSphere Client 上，NSX Controller 叢集平面可能會顯示內部 IP 位址 172.17.0.1，而不是實際 IP 位址
在 vSphere Client 上，NSX Controller 的 IP 位址誤顯示為 172.17.0.1，而不是實際 IP 位址。NSX Manager 的 IP 位址則正確顯示。

因應措施：不需要執行任何動作。這個表面性的問題並不會影響任何功能。

- 問題 1771626：不支援變更 NSX Controller 節點的 IP 位址

因應措施：重新部署 NSX Controller 叢集。

- 問題 1940046：在多個第 1 層邏輯路由器中新增相同的靜態路由並通告時，東-西向流量失效
在多個第 1 層邏輯路由器中新增相同的靜態路由並通告時，東-西向流量失效。

因應措施：首碼位於第 1 層分散式路由器已連線網路的後方時，應僅從起始的第 1 層邏輯路由器通告靜態路由。

- 問題 1753468：在橋接的 VLAN 上啟用跨距樹狀結構通訊協定 (STP) 會導致橋接器叢集狀態顯示為關閉
在用來與 LACP 整併橋接的 VLAN 上啟用 STP 時，實體交換器連接埠通道會被封鎖，而導致 ESX 主機上的橋接器叢集顯示為關閉。

因應措施：停用 STP，或啟用 BPDU 篩選器和 BPDU 保護。

- 問題 1753468：第 0 層邏輯路由器未彙總路由，而是由邏輯路由器個別加以重新分配
第 0 層邏輯路由器並未針對未涵蓋所有已連接之子首碼的首碼執行路由彙總，而是由邏輯路由器個別分配路由

因應措施：無。

- 問題 1536251：不支援將一個 ESX 主機中的虛擬機器複製到連結至相同邏輯交換器的另一個 ESX 主機
從一個 ESX 主機複製虛擬機器時，如果該虛擬機器已登錄於另一個 ESX 主機上，則第 2 層網路會失敗

因應措施：如果 ESX 主機是 Virtual Center 的一部分，則使用虛擬機器複製。

如果您在 ESX 主機之間複製了虛擬機器，則外部識別碼在虛擬機器 .vmx 檔案中必須是唯一的，第 2 層網路才能運作。

- 問題 1747485：從 LAG 介面中移除任何上行，將會使所有 BFD 通訊協定關閉，並翻動 BGP 路由
從已設定的 LAG 介面中刪除任何介面時，將會使所有 BFD 通訊協定關閉並翻動 BGP 路由，而對流量流向造成影響。

因應措施：無。

- 問題 1741929：在 KVM 環境中，如果設定了連接埠鏡像並啟用截斷，來自來源的 Jumbo 封包將會以片段傳送，但在鏡像目的地會重新組合

因應措施：不需要因應措施，因為重新組合會由目的地虛擬機器 vNIC 驅動程式執行。

- 問題 1619838：變更邏輯路由器對不同組邏輯交換器之傳輸區域連線的作業會因為不符錯誤而失敗
邏輯路由器對於下行連接埠僅支援單一覆蓋傳輸區域。因此，若未刪除現有的下行或路由器連結連接埠，即無法變更不同組邏輯交換器的傳輸區域連線。

因應措施：完成下列步驟。

1. 刪除所有現有的下行或路由器連結連接埠。

2. 等待一段時間，讓系統進行更新。
3. 重新嘗試變更不同組邏輯交換器的傳輸區域連線。

- 問題 1625360：在建立邏輯交換器後，NSX Controller 不一定會顯示新建立的邏輯交換器資訊

因應措施：在建立邏輯交換器後等待 60 秒，再於 NSX Controller 上查看邏輯交換器資訊。

- 問題 1581649：在建立和刪除邏輯交換器後，VNI 集區範圍無法縮小
範圍縮小失敗，因為 VNI 並未在邏輯交換器刪除後立即釋放。VNI 會在 6 個小時後釋放。這是為了防止 VNI 在其他邏輯交換器建立時被重複使用。因此，在邏輯交換器刪除後，您必須在 6 個小時後才能縮小或修改範圍。

因應措施：若要修改 VNI 為邏輯交換器配置的範圍，請在刪除邏輯交換器之後等待 6 小時。或者，請使用 VNI 集區中的其他範圍，或重複使用相同範圍而不要縮小或刪除範圍。

- 問題 1516253：Intel 82599 NIC 具有「已接收的佇列位元組計數器 (QBRC)」方面的硬體限制，會在已接收的位元組總計超過 0xFFFFFFFF 時導致溢位
由於有此硬體限制，在溢位發生時，`get dataplane physical-port stats` 的 CLI 輸出將不符合實際數目。

因應措施：執行 CLI 一次，讓計數器在較短的持續期間內重設及重新執行。

- 問題 2075246：不支援將第 1 層邏輯路由器從一個第 0 層邏輯路由器移到另一個。
將第 1 層邏輯路由器從一個第 0 層邏輯路由器移到另一個邏輯路由器會導致第 1 層邏輯路由器的下行連接埠路由連線中斷。

因應措施：完成下列步驟：

1. 從第 0 層邏輯路由器中斷連結第 1 層邏輯路由器。
2. 等待大約 20 分鐘，以便第 1 層邏輯路由器從第 0 層邏輯路由器完全中斷連結。
3. 將第 1 層邏輯路由器連結至另一個第 0 層邏輯路由器。
已還原下行連接埠路由連線。

- 問題 2077145：在某些情況下，嘗試強制刪除傳輸節點可能會導致孤立傳輸節點
使用 API 呼叫嘗試強制刪除傳輸節點造成問題，例如發生硬體故障且主機變得無法擷取、將傳輸節點狀態變更為孤立。

因應措施：刪除具有孤立傳輸節點的網狀架構節點。

- 問題 2099530：變更橋接器節點 VTEP IP 位址導致流量中斷
當橋接器節點 VTEP IP 位址變更時，在遠端 Hypervisor 上未更新從 VLAN 至覆疊的 MAC 資料表，導致流量中斷長達 10 分鐘。

因應措施：從 VLAN 起始流量變更，以便重新整理 Hypervisor 上的覆疊 MAC 資料表。

- 問題 2106176：在安裝的「正在等待登錄」步驟期間，NSX Controller 自動安裝會停止
使用 NSX Manager API 或 UI 執行 NSX Controller 自動安裝期間，其中一個進行中的 NSX Controller 的狀態會停止，且無限期顯示為正在等待登錄。

因應措施：完成下列步驟：

1. 傳送 API 要求以找出與停止的 NSX Controller 相關聯的虛擬機器識別碼。

`https://<nsx-mgr>/api/v1/cluster/nodes/deployments`

2. 傳送 API 要求以刪除停止的 NSX Controller。

`https://<nsx-mgr>/api/v1/cluster/nodes/deployments/<Controller id>?action=delete`

- **問題 2112459：取代橋接器叢集中的單一節點會造成流量捨棄**

當您取代橋接器叢集中的單一節點時，橋接的流量流向導致流量捨棄的舊節點，直到遠端 Hypervisor 中的轉送項目更新或過時為止。

因應措施：完成下列步驟：

1. 將取代節點置於橋接器叢集中。
2. 允許建立 HA。
3. 移除舊節點。

- **問題 216992：使用自訂邏輯連接埠 MTU 設定可能會導致封包捨棄**

使用邏輯連接埠上的自訂 MTU 設定時，例如邏輯路由器上行連接埠不合格值或第 0 層和第 1 層邏輯路由器的特定組態，可能會導致封包捨棄。預設 MTU 設定為 1500。

因應措施：使用預設 MTU 設定。

否則，不同邏輯連接埠上套用的 MTU 必須符合以下關聯性：

1. 將第 0 層邏輯路由器上行 MTU 設定為 8900。
2. 將 NSX Edge VTEP MTU 設定為 9000。
3. 將虛擬機器 MTU 設定為 8900。

第 0 層邏輯路由器和連線至第 0 層邏輯路由器的所有第 1 層邏輯路由器必須共置於相同的 NSX Edge 節點上。

- **問題 2125514：第 2 層橋接器容錯移轉後，某些 NSX Edge 虛擬機器上的邏輯交換器可能會對每個單一封包執行 BUM 複寫，直到重新學習 MAC**

第 2 層橋接器容錯移轉後，某些 NSX Edge 虛擬機器上的邏輯交換器可能會對每個單一封包執行 BUM 複寫將近 10 分鐘，直到為端點重新學習 MAC。端點產生下一個 ARP 後，系統復原本身。

因應措施：無

- **問題 2113769：在 NSX Edge VLAN 第 2 層橋接上不支援 DHCP 轉送**

透過 NSX Edge 上的第 2 層橋接連接埠將 VLAN 主機連線至邏輯交換器 VNI，導致邏輯路由器連接埠上的 DHCP 轉送代理程式不提供 IP 位址給 VLAN 主機。

因應措施：完成下列步驟：

1. 手動設定 VLAN 主機。
2. 將第 2 層橋接連接埠移至 ESXi 主機。

- **問題 2183549：在編輯集中式服務連接埠時，無法檢視新建立的 VLAN 邏輯交換器**

在管理程式 UI 中，您建立集中式服務連接埠和新的 VLAN 邏輯交換器後，如果您編輯集中式服務連接埠，則無法看到新建立的 VLAN 邏輯交換器。

因應措施：使用 API 來編輯連接埠。

- **問題 2160634：變更回送上的 IP 位址可以變更上行上的路由器識別碼的 IP 位址**

如果已變更回送上的 IP 位址，NSX Edge 會選取上行上的 IP 位址做為路由器識別碼。無法變更已指派為路由器識別碼的上行的 IP 位址。

對客戶的影響：1. 路由器識別碼的預期負面影響是所有 BGP 工作階段將不穩定。
2. 實際影響是路由器識別碼的變更可能導致偵錯 BGP 更困難，並且可能會導致混淆。

因應措施：停用 BGP 組態，並變更回送上的 IP 位址。

- **問題 2186040：如果傳輸節點不在系統中的前 250 個上行設定檔中，則會在使用者介面中停用實體 NIC**

的上行下拉式清單

如果傳輸節點不在系統中的前 250 個上行設定檔中，則會在使用者介面中停用實體 NIC 的上行下拉式清單。儲存傳輸節點導致從傳輸節點移除上行名稱。

因應措施：為該傳輸節點重新選取上行設定檔和上行名稱。

- 問題 2106635：建立靜態路由期間，變更 NULL 路由的管理距離會導致下一個躍點 NULL 設定從使用者介面中消失

建立靜態路由期間，如果您將下一個躍點設定為 NULL 且變更 NULL 路由的管理距離，下一個躍點 NULL 設定會從使用者介面中消失。

因應措施：重新選取下一個躍點。

安全服務已知問題

- 問題 1680128：用戶端與伺服器之間的 DHCP 通訊未加密

因應措施：使用 IPSEC 提高通訊的安全性。

- 問題 1711221：IPFIX 資料會透過網路以純文字格式傳送
依預設會關閉收集 IPFIX 流量的選項。

因應措施：無。

- 問題 1726081：Geneve 通道流量 (UDP) 在 KVM 中遭拒

因應措施：完成下列步驟：

如果 KVM 使用 firewalld，請使用下列命令在防火牆中建立一個開口：

```
# firewall-cmd --zone=public --permanent --add-port=6081/udp
```

如果 KVM 直接使用 Iptables，請使用下列命令建立開口：

```
# iptables -A INPUT -p udp --dport 6081 -j ACCEPT
```

如果 KVM 使用 UFW，請使用下列命令建立開口：

```
# ufw allow 6081/udp
```

- 當用戶端位於不同的網路且路由服務由客體虛擬機器提供時，DHCP 版本和更新封包不會到達 DHCP 伺服器

NSX-T 無法區分虛擬機器是否用作路由器，因此使用路由器虛擬機器路由傳送的單點傳播 DHCP 封包可能會遭到捨棄，原因是封包中的 CHADDR 欄位不符合來源 MAC。CHADDR 具有 DHCP 用戶端虛擬機器的 MAC，而來源 MAC 則來自路由器介面。

因應措施：如果虛擬機器的行為類似路由器，請在套用至路由器虛擬機器之所有 VIF 的交換器安全性設定檔中停用 DHCP 伺服器區塊。

- 問題 2108290：做為傳輸節點的裸機伺服器無法確保 NSX-T Data Center 的安全性功能

做為新類型傳輸節點的裸機伺服器不提供相同層級的安全性保證，例如微分割做為其他 Hypervisor 工作負載。這是因為在應用程式工作負載和 NSX 代理程式之間不會強制執行可靠信任界限。

因應措施：基於安全考量，請勿為承租人虛擬機器指派裸機伺服器的根權限，或以根使用者身分執行應用程式。如果承租人虛擬機器具有此類存取權，受到危及的承租人帳戶或應用程式可能會在裸機伺服器上執行惡意的活動，並導致 NSX-T Data Center 網路中的問題。

- 問題 2162722：權數索引不適用於「捨棄」或「拒絕」規則和無狀態規則

當流量叫用含「捨棄」/「拒絕」動作的規則或無狀態規則時，該規則的工作階段計數不能遞增，因為「工作階段」僅適用於可設定狀態的「允許」規則。權數索引將工作階段計數用作關鍵參數，因此它不會為針對此類規則變更。

因應措施：無

- 問題 2170512：如果介面具有 1,000 個以上規則，用於取得防火牆規則的 CLI 命令會失敗
如果介面具有 1,000 個以上規則，CLI 命令 `get firewall <VIF_ID> ruleset rules` 將傳回空字串。

因應措施：有 2 個因應措施：

- 改為執行命令「`nsxcli -c get firewall <VIF_ID> ruleset rules | json`」。
- 執行以下原始 CLI 命令。將顯示包含此結果的檔案名稱。
`ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules`

KVM 網路已知問題

- 問題 1775916：在 RHEL KVM 主機新增至網狀架構失敗之後，解析程式 API **POST /api/v1/error-resolver?action=resolve_error** 未解析錯誤

在 RHEL KVM 主機無法新增至網狀架構，且 NSX Manager 使用者介面將安裝狀態顯示為失敗之後，系統將會執行解析程式 API **POST /api/v1/error-resolver?action=resolve_error** 以解析錯誤。不過，重新將該主機新增至網狀架構時，會產生下列錯誤訊息：

無法在主機上安裝軟體。未處理的部署外掛程式執行動作。

安裝命令失敗。

因應措施：完成下列步驟。

1. 手動移除下列套件。

```
rpm -e glog-0.3.1-1nn5.x86_64
rpm -e json_spirit-v4.06-1.el6.x86_64
rpm -e kmod-openvswitch-2.6.0.4557686-1.el7.x86_64
rpm -e nicira-ovs-hypervisor-node-2.6.0.4557686-1.x86_64
rpm -e nsx-agent-1.1.0.0.0.4690847-1.el7.x86_64
rpm -e nsx-aggservice-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-cli-1.1.0.0.0.4690892-1.el6.x86_64
rpm -e nsx-da-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-host-1.1.0.0.0.4690932-1.x86_64 rpm -e nsx-
host_node_status_reporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-lldp-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-logical_exporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-mpa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-netcpa-1.1.0.0.0.4690924-1.el7.x86_64 rpm -e nsx-sfhc-
1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-support-bundle-client-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-transport_node_status-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsxa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e openvswitch-2.6.0.4557686-1.x86_64
rpm -e openvswitch-selinux-policy-2.6.0.4557686-1.noarch
rpm -e python-simplejson-3.3.3-1.el7.x86_64
```

如果在執行 `rpm -e` 命令時有任何錯誤，請在命令中加上 `--noscripts` 旗標。

2. 執行解析程式 API **POST /api/v1/error-resolver?action=resolve_error**。

3. 重新將 KVM 主機新增至網狀架構。

- 問題 1602470：在 KVM 上不支援負載平衡整併
- 問題 1611154：一個 KVM 傳輸節點中的虛擬機器無法聯繫位於另一個傳輸節點中的虛擬機器
有多個 IP 集區用於屬於不同網路的 VTEP 時，KVM 主機上的虛擬機器可能會無法聯繫在具有不同 IP 集區之 VTEP IP 位址的其他主機上部署的虛擬機器。

因應措施：新增路由，使 KVM 傳輸節點可聯繫其他傳輸節點上的 VTEP 所使用的所有網路。

例如，如果您有 25.10.10.0/24 和 35.10.10.0/24 這兩個網路，且本機 VTEP 的 IP 位址為 25.10.10.20，閘道為 25.10.10.1，則您可以使用下列命令為另一個網路新增路由：

```
ip route add dev nsx-vtep0.0 35.10.10.0/24 via 25.10.10.1
```

- 問題 1654999：底層流量的連線追蹤會減少可用的記憶體
在虛擬機器間建立大量連線時，可能會出現下列症狀。
在 /var/log/syslog 或 /var/log/messages 檔案中，您會看見如下的項目：
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950872] net_ratelimit: 239 callbacks suppressed
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950875] nf_conntrack: table full, dropping packet
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.958436] nf_conntrack: table full, dropping packet
問題似乎會在設定了預設防火牆規則時顯現。如果未設定防火牆規則，則不會顯現此問題 (例如：將邏輯交換器放在防火牆排除清單中)。
附註：上方的記錄摘要只是範例。日期、時間和環境變數可能隨著您的環境而不同。

因應措施：新增防火牆規則，在底層裝置的連接埠 6081 上停用 UDP 的連線追蹤。

以下是範例命令：

```
# iptables -A PREROUTING -t raw -p udp --dport 6081 -j CT --notrack
```

此命令應設定在開機期間執行。如果平台也啟用了防火牆管理員 (Ubuntu：UFW；RHEL：firewalld)，則應透過防火牆管理員設定對等的規則。請參閱相關的[知識庫 2145463](#)。

- 問題 2002353：不支援使用 Linux 網路管理員來管理 KVM 主機上行
NSX-T**Data Center**管理 KVM 主機上用於 N-VDS 的所有 NIC。針對這些上行啟用網路管理員時，會發生組態錯誤。

因應措施：對於 Ubuntu 主機，從網路管理員排除將用於 NSX-T**Data Center**的 NIC。

在 Red Hat 主機上啟用 NSX-T**Data Center** 之前，先將 /etc/sysconfig/network-scripts 中的 NIC 組態指令碼修改為 NM_CONTROLLED="no"。如果已針對主機啟用 NSX-T**Data Center**，請進行相同的指令碼修改，然後重新啟動主機的網路功能。

- 問題 2186045：在 KVM 上，依預設，logrotate 會每天執行一次，而不是每分鐘執行一次
在 KVM 上，如果記錄檔的大小超過一天中以其大小為基礎的輪替原則中定義的大小限制，它將無法輪替，直到 logrotate 執行的當天結束為止。因此，記錄檔大小可能大於定義的大小限制。

因應措施：執行下列步驟：

1. 建立新目錄 /etc/cron.minutes。
2. 使用下列內容建立 /etc/cron.minutes/logrotate 指令碼：
#!/bin/sh
/usr/sbin/logrotate /etc/logrotate.conf
3. 變更 /etc/cron.minutes/logrotate 的權限：
chmod 755 /etc/cron.minutes/logrotate

4. 將 cron.minutes 附加為 /etc/crontab 中的項目：

```
echo "* * * * * root cd / && run-parts --report /etc/cron.minutes"
>>/etc/crontab
```

負載平衡器已知問題

- 問題 2010428：負載平衡器規則建立與應用程式限制

在使用者介面中，您可以僅從虛擬伺服器建立負載平衡器規則。使用 REST API 建立的負載平衡器規則無法在使用者介面中連結到虛擬伺服器。

因應措施：如果您使用 REST API 建立了負載平衡器規則，請使用 REST API 將該負載平衡器規則連結至虛擬伺服器。使用 REST API 建立的規則現在會出現在使用者介面的虛擬伺服器中。

- 問題 2016489：選取伺服器名稱指示時，LCP 無法設定預設憑證

在伺服器名稱指示 (SNI) 中使用多個憑證識別碼以避免 LCP 略過預設憑證時，應先在憑證清單中設定預設憑證識別碼。

因應措施：預設憑證應位於 SNI 憑證清單中的第一個。

- 問題 2115545：啟用負載平衡器健全狀況檢查後，直接連線至後端伺服器集區成員可能會失敗

當負載平衡器已連結至邏輯路由器時，若集區成員使用邏輯路由器的上行進行連線，則連線至邏輯路由器下行的用戶端無法使用與健全狀況檢查相同的通訊協定存取集區成員。

例如，如果負載平衡器已連結至邏輯路由器 LR1 且已針對透過 LR1 上行連線的集區成員啟用 ICMP 健全狀況檢查，則 LR1 下行上的用戶端無法直接對這些集區成員執行 Ping 動作。但是，同一用戶端可以使用其他通訊協定 (例如 SSH 或 HTTP) 與伺服器進行通訊。

因應措施：在負載平衡器上使用不同的健全狀況檢查類型。例如，為了能夠對後端伺服器執行 Ping 動作，可以使用 TCP 或 UDP 健全狀況檢查，而不是 ICMP 健全狀況檢查。

- 問題 2128560：設定負載平衡器 SNAT 自動對應和健全狀況檢查可能會偶爾導致健全狀況檢查或連線失敗

為同一個伺服器集區設定負載平衡器 SNAT 自動對應和健全狀況檢查 (例如 TCP、HTTP、HTTPS 或 UDP)，可能會偶爾導致健全狀況檢查或連線至該伺服器集區失敗。

因應措施：使用 SNAT IP 清單，而不是 SNAT 自動對應。

附註：在 SNAT IP 清單模式下指定的 SNAT IP 位址不應包括邏輯路由器上行 IP 位址。

例如，如果負載平衡器連結至第 1 層邏輯路由器 LR1，則設定的 SNAT IP 範圍不應包括 LR1 上行 IP 位址。

解決方案互通性已知問題

- 問題 1588682：將 ESXi 主機置於鎖定模式，會停用使用者 nsx-user

當 ESXi 主機置於鎖定模式時，使用者 vpxuser 將是唯一能夠驗證主機或執行任何命令的使用者。NSX-T Data Center 依賴於另一個使用者 nsx-user 在主機上執行所有 NSX-T Data Center 相關的工作。

因應措施：不要使用鎖定模式。請參閱 vSphere 說明文件中的[鎖定模式](#)。

作業和監控服務已知問題

- 問題 1749078：刪除 ESXi 主機和對應的主機傳輸節點上的承租人虛擬機器後，刪除 ESXi 主機的作業會失敗

刪除主機節點的作業涉及重新設定不同的物件，而可能需要數分鐘或更久。

因應措施：等待數分鐘，然後重試刪除作業。視需要重複執行。

- 問題 1761955：在登錄虛擬機器後，無法將虛擬機器的 vNIC 連線至 NSX-T Data Center 邏輯交換器。如果使用現有的 vmx 檔案來登錄 ESXi 主機上的虛擬機器，登錄作業會忽略下列 vNIC 特定錯誤：

- 以無效的網路支援設定的 vNIC。
- 連線至 NSX-T 邏輯交換器之 vNIC 的 VIF 連結失敗。

因應措施：完成下列步驟。

1. 在標準 vSwitch 上建立暫時連接埠群組。
2. 將處於中斷連線狀態的 vNIC 連結至新的連接埠群組，並將其標示為已連線。
3. 將 vNIC 連結至有效的 NSX-T Data Center 邏輯交換器。

- 問題 1774858：在極少數情況下，NSX Controller 叢集在執行多日之後會變成非作用中狀態。當 NSX Controller 叢集變成非作用中狀態時，所有的傳輸和 NSX Edge 節點都會失去 NSX Controller 的連線，而且無法進行組態的變更。但資料流量不受影響。

因應措施：完成下列步驟。

- 修正現有的磁碟延遲問題。
- 在所有 NSX Controller 上重新啟動 cluster-mgmt 服務。

- 問題 1576304：捨棄的位元組計數未納入為連接埠狀態和統計資料報告的一部分。使用 /api/v1/logical-ports/<port-id>/statistics 或 NSX Manager 來檢視邏輯連接埠狀態和統計資料時，捨棄的封包計數值會是 0。此值不正確。無論捨棄的封包數量為何，此處顯示的數字一律會空白。

因應措施：無。

- 問題 1955822：授權使用量報告 csv 檔案也應包含 CPU 和虛擬機器權利，以及實際使用量。查詢授權使用量報告時 (透過 API/UI) 時，資料僅包含目前的使用量。

因應措施：透過 UI 或 REST API 查詢目前授權允許的使用量限制：

方法：GET; URI: /api/v1/licenses

- 問題 2081979：傳輸節點主機無法連線到任何控制器。NSX Proxy 記錄顯示下列內容。預期會顯示「憑證驗證」訊息，但是不存在。

```
TCP connection started: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757:1234
Doing SSL handshake
TCP connection established: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757,
local addr: 10.171.0.59:36048, remote addr: 10.171.0.73
```

因應措施：以管理員身分登入控制器，並執行下列命令：

```
set debug
get mediator forcesync
```

升級已知問題

- 問題 1930705：管理平面升級期間連線至邏輯交換器的虛擬機器 vMotion 失敗。在管理平面升級期間，嘗試對連線至邏輯交換器的虛擬機器執行 vMotion 會失敗。

因應措施：等候管理平面升級完成，然後重試 vMotion 處理程序。

- 問題 2005423：從舊版 NSX-T 升級的 KVM 節點不會自動變更為使用 balance-tcp。NSX-T 不會自動將升級後的 KVM 主機上行的繫結模式從主動備份修改為 balance-tcp。

因應措施：即使沒有任何組態變更，也請編輯傳輸節點，以更正模式設定。

- 問題 2101728：有時，NSX Edge 升級程序會在成功升級 NSX Edge 群組後暫停 NSX Edge 群組升級成功，但是，在第二個 NSX Edge 群組升級期間程序暫停。

因應措施：按一下繼續以繼續進行 NSX Edge 群組升級。

- 問題 2106257：從 NSX-T 2.1 升級至 NSX-T 2.2 的使用者授權合約 API 接受工作流程變更更新升級協調器後和升級現有主機之前，應呼叫接受使用者授權合約 API。

因應措施：無

- 問題 2108649：如果在將要執行升級的磁碟分割中有檔案或目錄開啟，升級會失敗避免將要升級之磁碟分割中的檔案或目錄保持開啟，例如 NSX Manager 或 NSX Controller，這會導致升級程序失敗。

因應措施：重新開機發生失敗的應用裝置並重新啟動升級程序。

- 問題 2116020：從 NSX-T 2.1 升級至 NSX-T 2.2 後，不會移除某些 Ubuntu KVM 已過時的套件從 NSX-T 2.1 升級至 NSX-T 2.2 後，不會移除下列 Ubuntu KVM 已過時的套件。

- nsx-host-node-status-reporter
- nsx-lldp
- nsx-logical-exporter
- nsx-netcpa
- nsx-support-bundle-client
- nsx-transport-node-status-reporter
- nsxa

因應措施：完成下列步驟。

1. 在 /etc/vmware/nsxa/ 目錄中建立暫存檔。

```
cd /etc/vmware/nsxa  
touch temp.txt
```
2. 列出所有 nsxa 套件目錄和檔案。

```
dpkg -L nsxa  
/etc/vmware/nsxa# ls
```
3. 移除下列套件。
 - a) `dpkg --purge nsx-lldp`
 - b) `dpkg --purge nsx-support-bundle-client`
 - c) `dpkg --purge nsx-transport-node-status-reporter`
 - d) `dpkg --purge nsx-logical-exporter`
 - e) `dpkg --purge nsx-netcpa`
 - f) `dpkg --purge nsxa`
 - g) `dpkg --purge nsx-host-node-status-reporter`
4. 確認下列目錄可用。

```
/etc/vmware/nsxa/
```
5. 從 /etc/vmware/nsxa/ 目錄移除 temp.txt 檔案。

```
rm -f temp.txt
```

- 問題 2164930：空白主機升級單位群組存在時，管理平面升級完成且顯示已暫停狀態空白主機升級單位群組存在時，整體管理平面升級狀態顯示為已暫停，且主機升級狀態不會標記為 100%。

對客戶的影響：如果客戶在升級期間有空白主機群組，則 MP 升級完成後，升級狀態將顯示為已暫停。

因應措施：升級管理平面之前，先刪除空白主機升級單位群組。

如果已升級管理平面，則刪除空白主機升級單位群組，然後使用 CLI 重新啟動 `install-upgrade service`。

- 問題 2097094：不支援在上傳期間取消升級服務包上傳
上傳升級服務包 .mub 檔案時，您無法取消上傳作業。

因應措施：等待升級服務包 .mub 檔案完成上傳。

- 問題 2122242：將 Ubuntu KVM 主機從 NSX-T 2.1 升級至 2.2 或 NSX-T Data Center 2.3 不會移除 `nsx-support-bundle-client` 套件

將 Ubuntu KVM 主機從 NSX-T 2.1 版本升級至更新版本 (NSX-T 2.2 或 NSX-T Data Center 2.3) 時，即使不再使用 `nsx-support-bundle-client` 套件，仍會安裝它。透過叫用命令 (例如 `/usr/bin/dpkg -l`)，使用者可以查看是否仍安裝了該套件。

因應措施：以根使用者身分登入並執行下列命令以手動移除套件：

```
# /usr/bin/dpkg --purge nsx-support-bundle-client
```

- 問題 2186957：升級後，ESXi 主機不會結束維護模式

如果叢集中只有一台主機且升級協調器上次嘗試將其置於維護模式失敗，升級後，ESXi 主機不會結束維護模式。

因應措施：手動使主機結束維護模式，或確保主機可以進入維護模式 (每個叢集必須至少具有 2 台主機)。

- 問題 2166207：從 NSX-T Data Center 2.2 升級至 NSX-T Data Center 2.3 (帶有 500 個 Hypervisor) 期間，整體升級程序可能會無限期處於 IN_PROGRESS 狀態

從 NSX-T Data Center 2.2 升級至 NSX-T Data Center 2.3 (帶有 500 個 Hypervisor) 期間，按一下 [暫停]，然後進行多個網頁瀏覽器重新整理後，整體升級程序可能會無限期處於 IN_PROGRESS 狀態。

因應措施：在 NSX Manager 上登入 NSX-T Data Center CLI。輸入命令 `install-upgrade` 重新啟動服務。

- 問題 2113681：如果在 NSX Edge 升級後，KVM 主機變得無法連線且發生故障，升級協調器會嘗試升級故障主機，而不會繼續升級 NSX Controller 節點

升級 KVM 主機和 NSX Edge，並在主機上解除安裝新的 RPM 然後安裝舊的 RPM 後，主機將在升級協調器中無法使用。因此，升級協調器會嘗試升級 KVM 主機，而不會繼續升級 NSX Controller 節點。

因應措施：重新整理升級協調器使用者介面，按一下主機索引標籤，並嘗試升級 KVM 主機。

您也可以略過 KVM 主機升級，開啟命令提示字元並輸入命令 `curl -i -k -u admin -X POST`

`https://<nsx-manager-ip-address>/api/v1/upgrade/plan?action=continue\&skip=true`

API 已知問題

- 問題 1605461：Syslog 中的 NSX-T API 記錄會顯示系統內部 API 呼叫。NSX-T 將使用者叫用的 API 呼叫和系統叫用的 API 呼叫都記錄至 Syslog

Syslog 中的 API 呼叫事件記錄並未顯示使用者直接呼叫 NSX-T API。您可以在記錄中看到 NSX Controller 和 NSX Edge API 呼叫，即便這些 NSX-T 應用裝置並沒有公開的 API 服務。這些私人 API 服務由 NSX-T CLI 之類的其他 NSX-T 服務所使用。

因應措施：無。

- 問題 1641035：POST/hpm/features/<feature-stack-name?
action=reset_collection_frequency> 的 Rest 呼叫不會還原覆寫統計資料的 collection_frequency
如果您嘗試使用此 REST 呼叫將收集頻率重設為其預設值，則它不會進行重設。
因應措施：使用 PUT /hpm/features/<feature-stack-name>，並將 collection_frequency 設為新值。
- 問題 1648571：隨需狀態和統計資料要求出錯，此情況會斷斷續續發生。HTTP 失敗代碼不一致在特定情況下，隨需要求會失敗。有時候，這些要求會因為 HTTP 500 錯誤而失敗 (而不是因為 HTTP 503 錯誤)，即便 API 呼叫在重試時成功了。
就統計資料 API 而言，逾時情況可能會導致假性的訊息路由錯誤記錄。之所以發生此狀況，是因為在逾時期間到期後傳回了回應。
例如，可能會發生如下的錯誤：java.lang.IllegalArgumentException: Unknown message handler for type
com.vmware.nsx.management.agg.messaging.AggService\$OnDemandStatsResponseMsg.
就狀態 API 而言，逾時情況 (回應在逾時之後傳回) 可能會導致快取提前更新。

因應措施：重試 API 要求。
- 問題 1963850：GET API 顯示以區分大小寫方式排序的項目
GET API 傳回依顯示名稱排序的項目時，排序會區分大小寫。

因應措施：無。
- 問題 2070136：處理大量資料的分散式防火牆 API 失敗
必須建立或更新超過 100 MB 的資料的分散式防火牆 API 失敗，並顯示錯誤碼 500 和指出交易失敗的訊息。API 通常涉及具有超過 1000 個規則的區段，每個規則涉及許多來源、目的地和套用至物件。

因應措施：建立或逐漸更新規則。
- 問題 1895497：API 中的負載平衡器演算法 SRCDESTMACIPPORT 無法運作
呼叫 API 來建立傳輸節點的上行設定檔與具有來源和目的地 MAC 位址、IP 位址及 TCP/UDP 連接埠的 LAG 將會失敗。

因應措施：無

NSX Policy Manager 已知問題

- 問題 2057616：將 NSX Policy Manager 從 NSX-T 2.1 升級至 NSX-T 2.2 期間，不支援的 NSService 和 NSGroup 不會傳輸
將 NSX Policy Manager 從 NSX-T 2.1 升級至 NSX-T 2.2 期間，不支援的具有乙太類型的 NSService 與具有 MAC 集合和邏輯連接埠成員資格準則的 NSGroup 不會進行傳輸。

因應措施：完成下列步驟。
 1. 在 NSX-T 2.1 中，移除並修改任何通訊項目中使用的具有乙太類型的 NSService。
 2. 移除並修改任何通訊項目中使用的具有 MAC 集合和邏輯連接埠成員資格準則的 NSGroup。
 3. 將 NSX Manager 從 NSX-T 2.1 升級至 NSX-T 2.2。
 4. 使用 CLI 升級 NSX Policy Manager。
- 問題 2116117：UI 中的 NSX Policy Manager 拓撲索引標籤會顯示資料連線失敗
UI 中的 NSX Policy Manager 拓撲索引標籤會顯示資料連線失敗，因為原則網域中的群組包含不支援的 ESXi 6.7 版本上主控的虛擬機器。

因應措施：無
- 問題 2126647：並行更新至 NSX Policy Manager 分散式防火牆導致覆寫

當兩個使用者同時編輯 NSX Policy Manager 分散式防火牆區段時，最後一個使用者所做的變更會覆寫之前其他使用者所做的編輯。

因應措施：恢復第一個使用者所做的分散式防火牆變更。儲存變更後，第二個使用者可以進行變更。

NSX Cloud 已知問題

- 問題 2112947：在 Cloud Service Manager (CSM) 中升級 NSX 代理程式時，部分執行個體可能會顯示為失敗
在 CSM 中升級 NSX 代理程式時，部分執行個體可能因使用者介面無回應而顯示為失敗。

因應措施：重新整理使用者介面。

- 問題 2111262：部署 PCG 時，您可能會看到錯誤：「閘道部署失敗: [錯誤碼: 60609] 非同步作業失敗，且佈建狀態為: 失敗。」或者「無法建立名為 nsx-gw 的閘道虛擬機器，閘道部署失敗。」
這是罕見事件，該事件由 Microsoft Azure 基礎結構導致。

因應措施：重新部署失敗的公用雲端閘道 (PCG)。

- 問題 2110728：如果您正使用 HA，但透過使用 --gateway 選項僅指定一個 PCG 的 DNS 名稱，在虛擬機器上安裝了 NSX 代理程式，則容錯移轉至次要 PCG 無法運作。
容錯移轉後工作負載虛擬機器無法連線至 PCG，因此 PCG 無法強制執行/實現虛擬機器上的任何邏輯狀態。

因應措施：在工作負載虛擬機器上安裝代理程式時，從不使用 --gateway 選項。使用 VPC 或 VNet 的 [閘道] 畫面中的值。如需詳細資料，請參閱《NSX-T Data Center 管理指南》中的〈安裝 NSX 代理程式〉。

- 問題 2071374：在某些 Linux 虛擬機器執行個體上安裝 NSX 代理程式時，可能會出現有關「nscd」的無害錯誤訊息
說明：在正在執行「nscd」的虛擬機器上安裝 NSX 代理程式時，您可能會看到類似以下內容的錯誤訊息：「sent invalidate(pwd) request, exiting」。在執行如 Ubuntu 14.04 或 16.04 的虛擬機器上會發生此問題

因應措施：由於 Linux 散發的已知錯誤，導致這些訊息出現。這些訊息是無害的，且不會影響 NSX 代理程式安裝。

- 問題 2010739：兩個公用雲端閘道 (PCG) 均顯示為待命
如果主要 PCG 無法在閘道上線期間連線至控制器，則這兩個閘道 (主要和次要) 將處於待命模式，直到控制器與閘道之間的連線還原。

- 問題 2121686：CSM 顯示例外狀況「伺服器無法驗證要求」。
您可能會在 CSM 中看到這個錯誤，原因是 CSM 應用裝置時間與 Microsoft Azure 儲存伺服器或 NTP 不同步。在此情況下，Microsoft Azure 擲回例外狀況「伺服器無法驗證要求」，它是不明確的，但 CSM 中會顯示相同的錯誤。

因應措施：同步 CSM 應用裝置時間與 NTP 或 Microsoft Azure 儲存伺服器時間。

- 問題 2092378：在 HA 模式下部署 PCG 時會顯示處於待命模式的兩個 PCG，雲端同步會顯示主要 PCG 處於作用中狀態
在私人網路中透過 CSM 在 HA 模式下部署 PCG 之後，會在已部署的 PCG 上看到待命/待命或作用中/作用中狀態達 1 小時。在此間隔期間，使用者似乎有一些 PCG 部署問題，並且可能處於不明狀態而無法繼續。

因應措施：執行下列操作：

1. 部署 PCG 後從 UI 重新同步帳戶，透過此作業，CSM 可擷取最新的資料，並顯示在 CSM 中。
 2. 如果重新同步後，CSM 仍顯示 PCG 處於錯誤狀態，請檢查 NSX Manager 中 PCG 的連線狀態。
 3. 如果連線顯示為「啟動」，而狀態仍不正確，請繼續偵錯 PCG。
- 問題 2119726：在 Microsoft Azure VNet 中部署 PCG 時，先前與虛擬機器相關聯的公用 IP 可能會錯誤地列為隨意使用。

如果先前指派了公用 IP 的虛擬機器現在已關閉電源，這些公用 IP 將不再與其相關聯。這是因為虛擬機器關閉電源一段時間後，Microsoft Azure 會將與其相關聯的公用 IP 解除關聯。Microsoft Azure 未明確定義這段時間。

*因應措施：*請勿在您的 VNet 中關閉 PCG 的電源。這會阻止公用 IP 與主要 PCG 的上行介面解除關聯。如果您必須關閉 PCG 的電源，請確保不會重複使用與 PCG 相關聯的公用 IP，且在 PCG 重新開啟電源後，它們會立即取得相同的公用 IP。

- 問題 2165915：NSX Cloud 支援含 kmod.x86_64 0:20-15.el7_4.6 的 Red Hat Enterprise Linux 7.4
NSX Cloud 不支援執行含 kmod-20-15.el7_4.6 之 Red Hat Enterprise Linux 7.4 的虛擬機器執行個體。此問題由 Red Hat 報告的錯誤所致：https://bugzilla.redhat.com/show_bug.cgi?id=1522994。

*因應措施：*更新至已修正此錯誤的 kmod 版本，以便成功安裝 NSX 代理程式。

- 問題 2102828：在 Microsoft Azure 部署中，從 NSX-T 2.2 升級至 NSX-T Data Center 2.3 期間和之後，公用雲端閘道 (PCG) 可能會無法運作。
在 Microsoft Azure 部署中，系統已從 NSX-T 2.2 升級至 NSX-T Data Center 2.3，在少數情況下，公用雲端閘道 (PCG) 可能無法在其介面上取得 IP 位址。在 PCG 升級期間可能會遇到此問題，其中 PCG 的升級程序似乎當機。如果管理員從 Microsoft Azure 入口網站重新啟動 PCG 應用裝置，此問題可能也將其本身顯現為非可運作 PCG。此問題不適用於第一次安裝 NSX-T Data Center 2.3 的新系統。

*因應措施：*從 Microsoft Azure 入口網站重新啟動您要升級的 PCG，然後在 Cloud Service Manager (CSM) 中，確認 PCG 和虛擬機器執行個體的狀態有效。

- 問題 2180531：具有核心 4.14 及更低版本的 Ubuntu 16.04 虛擬機器執行個體支援 NSX 代理程式
具有核心 4.14 及更低版本的 Ubuntu 16.04 虛擬機器執行個體支援 NSX 代理程式。NSX 代理程式將無法用於具有核心 4.15 及更高版本的 Ubuntu 16.04 虛擬機器執行個體。

此問題沒有因應措施

- 問題 2170445：從 NSX-T Data Center 2.2 升級至 NSX-T Data Center 2.3 之後，將不會為 Microsoft Azure PCG 正確設定 PCG HA 狀態
將 Microsoft Azure PCG 從 NSX-T 2.2 升級至 NSX-T Data Center 2.3 之後，PCG 的 HA 狀態不會按預期成為 [作用中/待命]。慣用 PCG HA 狀態顯示為 [同步]，非慣用 PCG HA 狀態顯示為 [作用中]。因此，升級後執行 HA 容錯移轉時，只有其中一個 PCG 具有有效狀態。

*因應措施：*在 NSX-T 2.2 中，先將 PCG 的上行主機交換器設定檔中的 MTU 更新為 1500，然後再開始升級至 NSX-T Data Center 2.3。

可使用 NSX Manager UI 或 NSX Manager REST API 完成此作業。

透過 UI，執行下列操作：

1. 移至網狀架構 > 設定檔
2. 選取名稱為「PCG-Uplink-HostSwitch-Profile」且說明為「PublicCloudGateway Uplink HostSwitch Profile」的設定檔
3. 按一下編輯，並將 MTU 值修改為 1500，然後按一下儲存
4. 開始從 NSX-T 2.2 升級至 NSX-T Data Center 2.3。

透過 REST API，執行下列操作：

1. 使用下列命令取得所有主機交換器設定檔：

```
curl -X GET \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles \
  -H 'authorization: Basic <AUTH ID>' \
  -H 'content-type: application/json'
```

2.識別名稱為「PCG-Uplink-HostSwitch-Profile」且說明為「PublicCloudGateway Uplink HostSwitch Profile」的主機交換器設定檔，並取得該設定檔的識別碼：

```
curl -X PUT \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles/<host-switch-profile-id> \
  -H 'authorization: Basic <AUTH ID>' \
  -H 'content-type: application/json' \
  -d '{
    "resource_type": "UplinkHostSwitchProfile",
    "description": "PublicCloudGateway Uplink HostSwitch Profile",
    "id": "<host-switch-profile-id>",
    "display_name": "PCG-Uplink-HostSwitch-Profile",
    "tags": [
      {
        "scope": "CrossCloud",
        "tag": "public-cloud-manager"
      },
      {
        "scope": "PcmId",
        "tag": "<Existing PCM ID>"
      },
      {
        "scope": "EntityType",
        "tag": "default"
      },
      {
        "scope": "CloudScope",
        "tag": "<Existing VPC/VNET name>"
      },
      {
        "scope": "CloudType",
        "tag": "<Existing cloud type>"
      },
      {
        "scope": "CloudVpcId",
        "tag": "<Existing Vpc/Vnet id>"
      }
    ],
    "transport_vlan": 0,
    "teaming": {
      "active_list": [
        {
          "uplink_type": "PNIC",
          "uplink_name": "uplink-1"
        }
      ],
      "policy": "FAILOVER_ORDER"
    },
    "overlay_encap": "GENEVE",
    "mtu": 1500,
```

```
"_revision": 1
}'
```

- 問題 2174725：已部署 PCG 的受管理 VPC/VNet 在 CSM 中顯示為未受管理。
已部署 PCG 的受管理 AWS VPC 或 Microsoft Azure VNet 在 CSM 中顯示為未受管理。

因應措施：重新啟動 CSM 應會解決此問題。

- 問題 2162856：Azure PCG 具有無效的 HA 狀態 (兩個均為作用中或均為待命)
當您在 AWS 中部署一對 PCG，然後部署另一對用於 Azure 的 PCG 時，Azure PCG 將具有無效的 HA 狀態 (兩個均為作用中或均為待命)。

因應措施：先將 PCM 建立的 PCG 的上行主機交換器設定檔中的 MTU 更新為 1500，然後再開始跨雲端升級至 NSX-T Data Center 2.3。從管理程式 UI，執行下列步驟：

- 移至 [網狀架構] > [設定檔]。
 - 選取名稱為「PCG-Uplink-HostSwitch-Profile」且說明為「PublicCloudGateway Uplink HostSwitch Profile」的設定檔。
 - 按一下「編輯」，將「MTU」值修改為 1500，然後按一下「儲存」。
 - 啟動升級工作流程。
- 問題 2102321：在高流量期間，某些 NSX Cloud 作業可能會在 Microsoft Azure 上執行緩慢。
NSX Cloud 的某些作業依賴於 Microsoft Azure ARM API，例如管理虛擬機器或將其退出 NSX 管理；或在虛擬機器上執行隔離動作。在尖峰時段，Microsoft Azure 可能會叫用指定訂閱的 API 限制，在此情況下，它將會啟動節流該訂閱的所有 API 要求。在此期間，可能無法及時完成上述 NSX 作業。當 Microsoft Azure 停止節流要求時，最終會完成這些作業。公用雲端閘道上的 PCM 記錄類似以下指示目前發生節流的內容「*Azure Resource Manager read/write per hour limit reached.Will retry in: x seconds*」

因應措施：等待直到 Microsoft Azure 節流停止。

- 問題 2189738：為線上 VPC 停用先前已啟用的隔離原則後，無法連線 AWS 工作負載虛擬機器。
如果透過啟用隔離原則部署 PCG，且稍後如果您停用隔離模式，此 VPC 中某些 NSX 管理的 AWS 工作負載虛擬機器無法與 PCG 進行通訊。

因應措施：將下列輸入規則新增至 AWS VPC 中的 NSX Cloud 安全群組：gw-mgmt-sg：

附註：當您基於安全考量再次啟用隔離原則時，請移除這些規則。

類型	通訊協定	連接埠	來源
CUSTOM-TCP	TCP	8080	VPC-CIDR
CUSTOM-TCP	TCP	5555	VPC-CIDR

- 問題 2188950：您使用 API 來擷取 PCG 清單時，會看到以下錯誤：「針對指定的識別碼找不到 VNet」。
如果從 CSM 刪除與部署的 PCG 相關聯的帳戶，則會看到此錯誤。

因應措施：在部署 PCG 所在的 CSM 中，新增 Microsoft Azure 帳戶。

- 問題 2191571：如果用於 PCG 部署的 SSH 公開金鑰並非以電子郵件識別碼結尾，則 PCG 部署不會啟動。
SSH 公開金鑰必須以電子郵件識別碼結尾，否則，PCG 部署將不會啟動並顯示錯誤。

因應措施：確保 SSH 金鑰結尾為電子郵件識別碼。

- 問題 2092073：在 Windows 工作負載虛擬機器上，不能正確接收 IPFIX 範本。

在 Windows 工作負載虛擬機器上，在與虛擬機器相同的子網路中設定 IPFIX 收集器後，不會立即傳出邏輯交換器和防火牆 IPFIX 範本。這是因為在傳出 UDP 封包之前，Windows 通訊端預期 IPFIX 收集器 IP 位址的 ARP 項目。如果遺失 ARP 項目，則會以無訊息方式捨棄所有 UDP 封包，最後一個封包除外。如此一來，在 IPFIX 收集器上，會接收不含任何範本資訊的資料封包。

*因應措施：*請執行下列其中一個動作：

- 使用以下命令為 IPFIX 收集器新增靜態 ARP 項目：

```
netsh interface ipv4 add neighbors "<Interface name>" <collector IP> <physical address of collector>
```

例如：

```
netsh interface ipv4 add neighbors "Ethernet 3" 172.26.15.7 12-34-56-78-9a-bc
```

- 在與工作負載虛擬機器不同的子網路上設定 IPFIX 收集器。

- 問題 2210490：如果您在 CSM 中新增 Proxy 設定檔，則獲指派以下任何角色的所有 CSM API 使用者均可看到密碼：雲端服務稽核員或雲端服務管理員。
如果您在 CSM 中建立 Proxy 設定檔，並提供使用者名稱和密碼，即使您無法在 CSM UI 中檢視密碼，它仍可見，以回應下列 API：

- /csm/proxy-server-profiles
- /csm/proxy-server-profiles/<profile-id>

- 問題 2039804：PCG 部署失敗，但不會在 AWS 中終止 PCG 執行個體。
如果您正在部署 PCG 但部署失敗，仍會看到 AWS VPC 中的 PCG 執行個體和 NSX Manager 中自動建立的邏輯實體。

*因應措施：*手動刪除自動建立的 NSX Manager 實體，並終止 AWS VPC 中的 PCG 執行個體。

NSX Container Plug-in (NCP) 已知問題

- PAS 2.1.0 CNI 變更

由於 PAS 2.1.0 中的 CNI 外掛程式變更，沒有 NSX-T 圖標 (無論版本是哪個) 將使用 PAS 2.1.0。在 PAS 2.1.1 中已修正此問題。

- 問題 2118515：在大規模設定中，NCP 需要花很長時間，在 NSX-T 中建立防火牆
在大規模設定 (例如，250 個 Kubernetes 節點、5000 個網繭、2500 個網路原則) 中，NCP 可能需要花幾分鐘時間，在 NSX-T 中建立防火牆區段和規則。

*因應措施：*無。建立防火牆區段和規則後，效能應會恢復正常。

- 問題 2125755：執行 Canary 更新和階段式輪流更新時，StatefulSet 可能會中斷網路連線
如果在 NCP 升級至目前版本之前已建立 StatefulSet，StatefulSet 可能會在執行 Canary 更新和階段式輪流更新時中斷網路連線。

*因應措施：*在 NCP 升級至目前版本後建立 StatefulSet。

- 問題 2131494：將入口類別從 nginx 變更為 nsx 之後，NGINX Kubernetes 入口仍然正常運作
當您建立 NGINX Kubernetes 入口時，NGINX 會建立流量轉送規則。如果將入口類別變更為任何其他值，即使您在變更類別後刪除 Kubernetes 入口，NGINX 也不會刪除規則，並且會繼續套用這些規則。這是 NGINX 的限制。

*因應措施：*若要刪除 NGINX 所建立的規則，請在類別值為 nginx 時刪除 Kubernetes 入口。然後，重新建立 Kubernetes 入口。

- 問題 2194845：不支援 PAS Cloud Foundry V3 API 功能「每個應用程式有多個程序」

當使用 PAS Cloud Foundry V3 API `v3-push` 來推送具有多個程序的應用程式時，NCP 不會為預設程序以外的程序建立邏輯交換器連接埠。NCP 2.3.0 及更早版本中會出現此問題。

因應措施：無

- 問題 2193901：不支援單一 Kubernetes 網路原則規則的多個 PodSelector 或多個 NsSelector 套用多個選取器僅允許來自特定網域的傳入流量。

因應措施：改為在單一 PodSelector 或 NsSelector 中搭配使用 matchLabels 和 matchExpressions。

- 問題 2194646：NCP 關閉時，不支援更新網路原則
如果 NCP 關閉時您更新網路原則，NCP 恢復運作時，網路原則的目的地 IP 集會不正確。

因應措施：NCP 啟動時，重新建立網路原則。

- 問題 2192489：停用 PAS 導向器組態中的「BOSH DNS 伺服器」後，Bosh DNS 伺服器 (169.254.0.2) 仍會顯示在容器的 `resolve.conf` 檔案中。
在執行 PAS 2.2 的 PAS 環境中，停用 PAS 導向器組態中的「BOSH DNS 伺服器」後，Bosh DNS 伺服器 (169.254.0.2) 仍會顯示在容器的 `resove.conf` 檔案中。這會導致具有完整網域名稱的 Ping 命令花費很長時間。PAS 2.1 不存在此問題。

因應措施：無。此為 PAS 問題。

- 問題 2194367：NSX-T 圖標不適用於部署自己路由器的 PAS 隔離區段
NSX-T 圖標不適用於部署自己 GoRouters 和 TCP 路由器的 Pivotal 應用程式服務 (PAS) 隔離區段。這是因為 NCP 無法取得路由器虛擬機器的 IP 位址，並建立 NSX 防火牆規則以允許從路由器至 PAS 應用程式容器的流量。

因應措施：無。

- 問題 2199504：NCP 建立的 NSX-T 資源的顯示名稱限制為 80 個字元
當 NCP 在容器環境中為資源建立 NSX-T 資源時，它會透過組合叢集名稱、命名空間或專案名稱和容器環境中的資源名稱，來產生 NSX-T 資源顯示名稱。如果顯示名稱長於 80 個字元，將被截斷為 80 個字元。

因應措施：無

- 問題 2199778：在 NSX-T 2.2 中，不支援名稱長度超過 65 個字元的入口、服務和密碼
在 NSX-T 2.2 中，將 `use_native_loadbalancer` 設定為 `True` 時，類型為 LoadBalancer 的入口和服務參考的入口、密碼和服務的名稱長度必須小於或等於 65 個字。否則，入口或服務將無法正常運作。

因應措施：設定入口、密碼或服務時，指定長度為小於或等於 65 個字元的名稱。

- 問題 2065750：安裝 NSX-T CNI 套件失敗，並顯示檔案衝突
在安裝了 Kubernetes 的 RHEL 環境中，如果您使用 `yum localinstall` 或 `rpm -i` 安裝 NSX-T CNI 套件，會看到錯誤，指示與 `kubernetes-cni` 套件中的檔案衝突。

因應措施：使用命令 `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm` 安裝 NSX-T CNI 套件。

- 對於類型為 ClusterIP 的 Kubernetes 服務，不支援以用戶端 IP 為基礎的工作階段相似性
對於類型為 ClusterIP 的 Kubernetes 服務，NCP 不支援以用戶端 IP 為基礎的工作階段相似性。

因應措施：無

- 對於類型為 ClusterIP 的 Kubernetes 服務，不支援 hairpin-mode 旗標
對於類型為 ClusterIP 的 Kubernetes 服務，NCP 不支援 hairpin-mode 旗標。

因應措施：無

- 問題 1372211：兩個介面位於相同子網路上

如果通道端點位於與管理介面相同的子網路上，通道流量即可能外流至管理介面。之所以發生此狀況，是因為通道封包可能經過管理介面。請確定管理介面位於與通道端點介面不同的子網路上。